Reinforcing Security, Privacy, and Civil Liberties

The United States has long been a beacon for democracy around the world. Strengthening our homeland security ensures that our way of life and the rights bestowed by the U.S. Constitution remain intact. As the Administration develops and employs new technologies and gathers information from the private sector for our homeland security efforts, it must ensure that our society's constitutional guarantees relating to privacy, due process, and civil liberties are protected.

The protection of our nation's civil liberties and privacy is fundamental to the American way of life. Our homeland security efforts are, after all, designed to preserve the "unalienable rights that are essential to the strength and security of our nation: life, liberty, and the pursuit of happiness."[1] As the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (the Gilmore Commission) found in 2003, "security" and "civil liberties" are mutually reinforcing parts of the effort to strengthen our homeland.[2]

The development of homeland security initiatives requires our government to protect fundamental constitutional rights and to strive to minimize unnecessary impositions on the freedoms and privileges enjoyed in the United States. The Gilmore Commission found that "[g]overnments must look ahead at the unintended consequences of policies in the quiet of the day instead of the crisis of the moment."[3] As our government develops post 9/11 homeland security initiatives in areas such as immigration, intelligence collection, law enforcement, and the use of new technologies it should thoughtfully and carefully review their impact on our fundamental freedoms.

Our first obligation is to pay close attention to the law enforcement and other authorities the government acquires in the name of fighting terrorism. Congress passed the USA PATRIOT Act in response to the attacks of September 11. The Act increased the ability of law enforcement and intelligence agencies to more effectively share information about terrorists and their activities, broadened federal authority to track and intercept communications for both law enforcement and foreign intelligence gathering purposes, provided for the detainment and deportment of alien terrorists, and added resources to fight terrorism financing. While some parts of the USA PATRIOT Act have provided important counterterrorism tools, concerns have been expressed that other sections of the legislation extend overly intrusive authorities to the government. Congress wisely provided that certain wiretapping and foreign intelligence provisions would expire after four years so that the efficacy of these provisions and their impact on personal liberty could be carefully assessed. Our country should have this important debate, as the Gilmore Commission put it, "in the quiet of the day," before moving to extend the expiration date of these provisions.

---

[1] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, also known as the Gilmore Commission, *Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty*, December 2003, http://www.rand.org/nsrd/terrpanel/volume_v/volume_v_report_only.pdf.

[2] Ibid.

[3] Ibid.

Our country needs to have a national discussion as well on how innovative technologies and information sharing and collection systems should be used to protect the homeland. Technology gives federal agencies the capability to access homeland security information in a cohesive manner, regardless of whether that information is held in databases and networks at different agencies, thereby increasing the likelihood that we can identify potential terrorists. In doing so, however, the government should ensure that information is accurate, remains confidential, and that access is limited to only appropriate personnel so as to protect civil liberties and privacy. Given the sensitivity of information gathered about individuals, it is also imperative that this data be protected during its creation, transmission, and storage.[4]

Likewise, if the government uses information that is held by the private sector, it should do so within a system of rules and guidelines that protect civil liberties. In today's technology-dependent, transaction-friendly society, Americans produce millions of records of their daily activities – ranging from credit card purchases to government registration and accounting systems to logs of personal time spent on the Internet and in entertainment venues. Unchecked access to such information by the government and other entities without sufficient cause could violate many of our constitutional rights.

In addition, voluntary disclosure of personal customer information gathered by private sector entities to government agencies for data-mining projects - without notification to those customers - continues to raise concerns. For example, in September 2003 JetBlue admitted that it had given five million passenger itineraries, possibly through the assistance of the Transportation Security Agency (TSA), to a defense contractor as part of a study seeking ways to identify high risk customers.[5] More recently, Northwest Airlines admitted that it handed over three months of passenger records to the National Aeronautics and Space Administration in 2001 for a data mining project. These disclosures were done without notification to customers, almost all of whom are presumably law-abiding individuals with no connections to terrorists. Consequently, the Federal Trade Commission and the Departments of Defense and Homeland Security are investigating the JetBlue disclosure, while two class action lawsuits have been filed against Northwest claiming that the airline illegally shared the private information.[6]

In the past year, several homeland security initiatives have been derailed or postponed because the Administration has failed to adequately evaluate the programs' effects on privacy and civil liberties. The Terrorism (first known as Total) Information Awareness (TIA) project, an initiative within the Defense Advanced Research Project Agency's Information Awareness Office, exemplifies the problem of developing programs without fully considering their impact on individual privacy. The program was designed to analyze as much information as possible on individuals and use computers and human analysis to detect potential terrorist activity. It planned to search existing databases containing information such as financial records, medical records, communication records, and travel records to find matches for particular patterns.[7] Concerns

---

[4] Markle Foundation's Task Force on National Security in the Information Age, *Protecting America's Freedom in the Information Age*, October 2002, and *Creating a Trusted Network for Homeland Security*, December 2003.

[5] Thomas Claburn, "Northwest CEO Urges Airline Execs To Talk Privacy," *Information Week*, January 22, 2004, http://www.informationweek.com/story/showArticle.jhtml?articleID=17500687.

[6] Ryan Singel, "Army Quietly Opens JetBlue Probe,"*Wired*, November 26, 2003, http://www.wired.com/news/privacy/0,1848,61374,00.html.

[7] Defense Advanced Research Projects Agency, *Report to Congress regarding the Terrorism Information Awareness Program In Response to Consolidated Appropriations Resolution, 2003, Public Law 108-7, Division M, § 111(b)*, May 20, 2003, http://www.darpa.mil/body/tia/tia_report_page.htm

regarding civil liberties and privacy led to TIA's cancellation, with Congress eliminating the Information Awareness Office responsible for creating the program.

Concerns are also raised by the Computer Assisted Passenger Prescreening System (CAPPS) II, which uses databases to check airline passengers' backgrounds and scores them on their potential to be risks. Various civil liberties and privacy issues have been identified with CAPPS II, including the lack of safeguards in place to protect passengers wrongly identified as terrorists, as well as questions regarding whether adequate security protections are in place to keep hackers and other criminals from accessing the personal information of passengers. As a result, Congress mandated that the program not be deployed until the General Accounting Office (GAO) completed a privacy and civil liberties assessment of the program.[8] The GAO report, released on February 12, was inconclusive on TSA's privacy efforts. The report found that "[u]ntil TSA completes its privacy plans and the program is further developed," it could not be determined if the agency had identified all of the privacy risks and necessary mitigation efforts.[9]

Some of these projects might have been successfully implemented if civil liberties and privacy had been given great attention during their development. Benjamin Franklin once said "they that would give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." Our government should strive to be better in its implementation of new programs to protect our homeland, as Americans deserve both their liberty and safety.

SECURITY GAP: There is No Framework in the Government for Evaluating the Security and Privacy of New Technologies.

In a 2003 report, the Markle Foundation's Task Force on National Security in the Information Age found that the government lacked a "systematic effort to consider the privacy implications of the proposed programs or to develop an overall policy framework that would govern the deployment of new technologies."[10] To protect civil liberties, a framework should be in place that the government can use to secure new technologies and develop privacy-protecting processes. To effectively combat terrorism and protect privacy, a framework establishing clear policies and guidelines is needed to "identify the types of databases involved, define the purposes of the data review, and clarify the authorization for collecting and disseminating whatever is found."[11] Such a framework could assist the government's homeland security efforts, allowing it to use technology to better manage and sort the large amount of data it gathers.

A framework also can help us ensure that databases used across the government operate within federal privacy laws and do not offend our constitutional values. Protecting our homeland and protecting our citizen's privacy should not be a "balancing act" where one is sacrificed for the benefit of the other. Rather, homeland security and privacy should reinforce one another through safeguards that build oversight and restraints on the misuse of power into our security initiatives.

---

[8] Judi Hasson, "Congress Demands Study of CAPPS II," *fcw.com*, September 26, 2003, http://www.fcw.com/fcw/articles/2003/0922/web-capps-09-26-03.asp.

[9] U.S. General Accounting Office, *Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, February 13, 2004, Available at http://www.gao.gov.

[10] Markle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security*, December 2003, 14.

[11] Markle Foundation Task Force on National Security in the Information Age, *Protecting America's Freedom in the Information Age*, October 2002, 36.

Technology has advanced significantly, with the advent of biometrics, supercomputing, interconnected global networks, the Internet, and other new technologies. Indeed, a bipartisan proposal by former government officials from the Clinton and Reagan administrations found that to properly protect our citizen's privacy the federal government should take into account "the revolutionary changes in recent years in communication, surveillance and database technology, and the implications of those changes for individual privacy and personal liberties."[12]

Unfortunately, the federal government has not conducted a comprehensive assessment of the use of new technologies and privacy in 30 years. The original Privacy Act of 1974 established the "U.S. Privacy Protection Study Commission" to evaluate the statute and issue a report on how to improve privacy protections. The Commission issued its report "Personal Privacy in an Information Society" in 1977 and ceased its operations. Since that time, there has not been a comprehensive national government-wide effort to evaluate the privacy implications of new technologies.

SECURITY RECOMMENDATION

To secure our nation, we should create an environment that protects sensitive information and individual civil rights.[13] By defending civil liberties we can strengthen our homeland defense and our country. In order to ensure that a comprehensive privacy and homeland security evaluation is completed, the Administration should create a new Commission on Privacy, Freedom, and Homeland Security.[14] This Commission would be charged with evaluating how we can organize our homeland security efforts in a manner that protects our nation and civil liberties and privacy in accordance with the fundamental values of our country. The Commission would create a comprehensive framework on the use of new technologies for homeland security that can provide guidance to the federal government on evaluating the purpose behind new technologies, the treatment of information gathered on individuals, and the access and distribution of information that might be gathered. The Commission would establish safeguards and protections for government access to and the use of individuals' personal information from commercial databases and lists. In particular, the Commission would devise mechanisms by which individuals could challenge and correct mistakes in databases that are utilized by the federal government. The Commission would also assess federal and state privacy statutes, evaluating how those laws are helping or hindering the protection of our homeland.

SECURITY GAP: Private Databases are Being Shared With the Government Without Customer Notification.

In January, the Department of Homeland Security (DHS) announced that it will require all airline carriers and reservation companies to submit personal information collected about their customers to the government as part of the CAPPS II program. Currently, airlines are not legally required to

---

[12] Peter Swire and Jeffrey Eisenach , "Ensuring privacy's post-attack survival," *Zdnet.com*, September 11, 2002, http://zdnet.com.com/2100-1107-957464.html.

[13] Markle Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security*, December 2003, 44.

[14] Peter Swire and Jeffrey Eisenach , "Ensuring privacy's post-attack survival," *Zdnet.com*, September 11, 2002, http://zdnet.com.com/2100-1107-957464.html.

notify customers that they may submit passengers' personal information to the government for screening and analysis.

SECURITY RECOMMENDATION

Private sector entities that share with the federal government personal information of their customers held in commercial databases should be required to notify their customers of that fact, so long as that disclosure does not affect ongoing civil or criminal investigations. For example, airline carriers and reservation companies should be required, at the time of ticketing, to let customers know that their information will be turned over to the federal government as part of programs such as CAPPS II. In addition, procedures should be in place to allow customers to correct erroneous information about themselves in databases that might be shared with the federal government.

SECURITY GAP: The Government Lacks Essential Privacy Office.

The Administration is not doing enough to evaluate and protect civil liberties and the Constitution in today's environment of new technologies and new security concerns, as demonstrated by the controversies surrounding TIA, the Jet Blue disclosure, and CAPPS II. This is partly due to the fact that the Administration has neither a single office within the federal government responsible for evaluating privacy issues within the government nor designated officers within every agency to review privacy issues.

In 1998, President Clinton required every agency to "designate a senior official within the agency to assume primary responsibility for privacy policy."[15] The next year, he created a "chief counselor for privacy" position for the federal government within the Office of Management and Budget (OMB) to advise on privacy issues. The counselor reviewed proposals before they went public and when there were privacy problems fixed them before the proposals were implemented.[16] The privacy counselor position was eliminated, however, at the beginning of the current Administration. Many of the privacy leaders within the federal agencies left the government and were not replaced.[17] No senior official within the White House or OMB has been designated to evaluate privacy in new technologies throughout the federal government.

Recognizing the need to have someone responsible for privacy relating to homeland security programs, Congress required DHS to create a "privacy office," tasking it with the following:

- Ensuring that DHS complies with the Privacy Act of 1974;
- Adequately considering privacy when DHS collects, uses, and discloses personal information; and

---

[15] William J. Clinton, *Memorandum for the Heads of Executive Departments and Agencies*, May 14, 1998, http://www.cdt.org/privacy/survey/presmemo.html.

[16] William Matthews, "Privacy Czar Plays Homeland Role," *Federal Computer Week*, November 21, 2002, http://www.fcw.com/fcw/articles/2002/1118/web-private-11-21-02.asp.

[17] U.S. House, Committee on the Judiciary, Subcommittee on Commercial and Administrative Law, *Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security*, February 10, 2004.

- Properly assessing the impact of its practices and rules on privacy.[18]

The privacy office, however, is only responsible for evaluating the privacy of programs within DHS. Many of the technologies, information sharing, and gathering mechanisms relating to homeland security are being implemented by the Administration in agencies other than DHS. The result is that there is no comprehensive and uniform evaluation of homeland security privacy issues in the federal government, especially in light of the elimination of the privacy counselor position within the White House. Without a single, accountable senior official to ensure that homeland security programs are evaluated in a uniform manner, our nation's privacy and civil liberties are at risk.

SECURITY RECOMMENDATION

The Administration should move promptly to name a person responsible for government-wide leadership on privacy issues. The government should create a Chief Privacy Officer responsible for evaluating privacy-related issues that arise in the information age, including those relating to the Privacy Act and the use of new technologies and information sharing mechanisms. In addition, the Administration should consider creating offices similar to the DHS privacy office in other agencies that handle large amounts of sensitive information, including the Departments of Treasury, Health and Human Services, the Social Security Administration, and the Department of Justice.

[18] Roy Mark, "Homeland Security Names First Privacy Czar," *dc.internet.com,* April 17, 2003, http://dc.internet.com/news/article.php/2192521.